EXHIBIT 526

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

AUTHENTICOM, INC., Plaintiff, v. CDK GLOBAL, LLC, and THE REYNOLDS AND REYNOLDS COMPANY, Defendants.	No. 3:17-CV-318-JDP

DECLARATION OF MALCOLM THORNE

I, Malcolm Thorne, hereby declare as follows:

1. I am the former Executive Vice-President & Chief Global Strategy Officer of CDK Global, LLC ("CDK"). I held that position from July 2014 until April 2017. I currently serve in a consulting role for the company.

2. While in my position as Executive Vice-President & Chief Global Strategy Officer, I was responsible for the company's entire strategic plan including the organization's rebranding and re-launch after its spin-off from ADP, as well as a series of key strategic initiatives, including the company's SecurityFirst initiative.

3. Prior to taking my EVP role, I was CDK's (ADP's) Vice-President, Product Management, Strategy, Marketing and Business Development from July 2011 to June 2014. Before that I was a consultant to the Senior Vice-President and CEO of ADP's Dealer Services Group (what is now CDK) from June 2010 to June 2011.

4. Before re-joining CDK in 2011, I was a Lecturer at the University of Wisconsin Madison Business School, teaching marketing and strategy. And before that I was the CEO of AutostyleMart, an automotive startup company, from May 2006 to October 2008.

5. Prior to 2006, I served in a number of positions in ADP's Dealer Services organization and before that owned my own company, Automotive Directions.

6. CDK was formerly the Dealer Services business of Automatic Data Processing, Inc. ("ADP"). In the Fall of 2014, CDK was spun off from ADP and became an independent publicly-traded company.

7. CDK licenses dealer management systems ("DMS") to automobile dealers. The DMS is essentially an enterprise software system that dealerships use to manage many critical aspects of their business.

8. Third-party application providers ("vendors") use data that is stored on the DMS to provide applications to dealerships that assist with various ancillary functions such as marketing, appointment management, and inventory. Vendors sometimes obtain that data through intermediary companies ("integrators") that extract the data from the DMS without the permission of the DMS provider.

9. Authenticom is an integrator that has hostilely extracted, and continues to try to extract, data from CDK's DMS in violation of CDK's contracts with its dealers and CDK's security policies.

10. Historically, integrators have extracted data from the DMS by obtaining user login credentials from the dealerships. While this process was widely tolerated by DMS providers—including CDK—two decades ago, changes in the industry have necessitated a shift to a more secure method of accessing data on the DMS.

11. CDK (and formerly ADP) has recognized for decades that finding the proper balance between DMS security and third-party integration is critical to its success as a DMS provider.

12. Security of the DMS and the data that resides on it was a concern for ADP as early as the 1990s. CDK's (and before that ADP's) contracts with its dealers have expressly prohibited third-party access to CDK's DMS platform using dealer log-in credentials since the mid 1990s. Def. Exs. 4-10.

13. But CDK acknowledged vendors' legitimate need for access to data on the DMS in order to provide applications to the dealerships. To facilitate secure access to the DMS platform by third-party vendors and applications providers who required DMS data to provide services to dealers, ADP established a third-party access program in the early 2000s. The program was generally known as the "3PA" program and was singularly focused on providing a reliable, secure interface with the DMS. Potential vendors that wanted to participate in the 3PA program submitted applications that were reviewed by a committee who ultimately determined whether to allow access and, if so, what level of access was appropriate and the corresponding cost of that access.

14. Eventually CDK (then ADP) realized that its security policies, proactive dealer education program and offerings (including working with the NADA on security initiatives for several years), were not influencing dealer behavior at a rapid enough pace. This lack of adoption by the dealers and CDK's somewhat lenient enforcement of its third party access policies compounded the high risks and costs to CDK of an unsecured method of accessing DMS. As these risks and costs became more evident, CDK affirmatively moved to address them. Concurrently, the National Auto Dealers Association ("NADA"), one of the largest

automobile dealer associations in the United States, began to issue warnings to dealers about the risks of sharing user IDs with third-party integrators. Defs. Ex. 20.

15. In 2013, NADA issued a memorandum to its members urging dealers to consider adopting stringent third-party access and security principles. Defs. Ex. 15.

16. In 2013, ADP also stepped up its efforts to warn dealers of risks associated with third-party access to data on the DMS. ADP published a brochure warning that third-party data access is like "giving the keys to your most valuable asset" and "should be done with careful planning." Defs. Ex. 21. ADP admonished dealers to "Never allow third parties to use your user ID or 'screen-scrape' your data." *Id.* Eventually, ADP decided that it would no longer recognize or approve the use of dealer usernames and passwords as an authorized method of third-party access. Defs. Ex. 22.

17. When I stepped into my position as EVP, I began an overall strategy and security review of CDK's entire 3PA ecosystem. As part of that analysis, and with the impending spin-off of CDK as an independent publicly traded company, securing the DMS and enforcing robust data security policies became and even larger priority for CDK.

18. Multiple factors influenced the shift in CDK's enforcement of its data security policies over the last decade.

19. First and foremost, was the concern about size and scope of the harm if CDK were to become the victim of a cybersecurity attack.

20. The size and scope of CDK's DMS ecosystem—as well as the type and amount of data stored on that system—has expanded significantly since it was first marketed over 40 years ago.

21. CDK currently manages an ecosystem that has some 40,000 installations of approved vendor applications and an average of more than 4.8 million transactions a day. Defs. Ex. 23.

22. CDK's DMS currently experiences 20,000 connections a day and manages and supports 1-2 Terabytes of data on a daily basis from 250+ 3PA partners. *Id.*

23. The average dealership has over 50,000 consumer records. *Id.*

24. Given CDK's evolving DMS platform, as part of my review of the original 3PA program and with the involvement and participation at all levels of management, including at the Board level, the company began to confront the reality that a data security breach of a CDK-dealer could be extremely costly and could harm both the dealers' brand and CDK's brand.

25. Along with the growing size and complexity of the DMS and the data stored therein, there was a renewed global and industry focus on legal and regulatory data security issues.

26. In its 2013 memorandum to its members, the NADA warned dealers that when their data was accessed by third-party integrators the dealers risked violating the Gramm-Leach-Bliley Act, which requires that third party service providers only access data that is needed to provide that service. Because unauthorized third-party integrators (such as Authenticom) often apply a standard set of search queries to all dealers, the data accessed is not limited to the information that a particular vendor requires for a particular customer.

27. Shortly after the NADA's memorandum, a series of high-profile data breaches in other industries (including retail and banking) focused our attention even more on security issues.

28. Generally speaking, we recognized that the auto industry—which represents approximately 3.5% of the U.S. GDP—was just as vulnerable as the retail and banking industries. *Id.*

29. The fact that CDK somewhat lagged behind it peers on third-party access security issues exacerbated the need to develop a comprehensive security program. In 2014, CDK was somewhat of an outlier in that even though it was the largest DMS provider, it was not considered "secure" by the industry. Defs. Ex. 24.

30. Mindful of the increased regulatory and industry focus on data security, and cognizant of the rise in severe data breaches in other industries, in January 2015, CDK engaged PricewaterhouseCoopers ("PwC") to conduct an assessment of its security program.

31. PwC concluded that CDK faced an "[i]ncreased risk exposure from not knowing or assessing all vendors that have access to CDK facilities, assets and data" and recommended that CDK close its DMS system to eliminate the security risks presented by hostile third-party access. Defs. Ex. 25.

32. As result of heightened awareness of legislation related to consumer security data and NADA security guidelines/recommendation, dealers began focusing on data security .

33. Dealers began requesting access accountability as well as solutions to help better manage the flow of data between themselves and third-parties. Defs. Ex. 24; *see also* Defs. Ex. 19.

34. CDK couldn't always give dealers the requested support because when dealers gave login credentials to unauthorized third-party integrators, such as Authenticom, there are no limits on the database elements that can be accessed and CDK has no way to audit what data is accessed or written back or who it is being sent to.

35. We realized that dealers believed "that DMS providers [were] under-serving them from a data security perspective," which could become "a key selection criterion for DMS purchase." Defs. Ex. 24.

36. This led us to conclude that if CDK helped dealers understand data security, the risks and benefits to their dealerships, and equipped them with information, tools, and services to protect their DMS data, then dealers might be more likely to partner with CDK to protect their data and secure the DMS.

37. In addition to data security concerns, several other factors including operational integrity, a willingness to expand program access, a desire to invest in real-time integration technology, and a goal of better protection of CDK's intellectual property impacted CDK's decision to dedicate itself to improving the overall 3PA program by, among other things, not permitting unauthorized third-party access to the DMS.

38. As more and more vendors began requiring access to CDK's DMS, operational integrity and the associated costs and client satisfaction issues became of particular importance.

39. A review performed by ADP in 2013 had shown that *all* 2,980 DMS systems examined had some data corruption issues, many of which were attributable to unauthorized thirty-party vendors and were causing problems for those same vendors because "their integration fails when it encounters data corruption." Defs. Ex. 26.

40. Using dealer login credentials, unauthorized third-parties have virtually unchecked access to pull any data from the system and write back whatever they wanted to add to the DMS. This hostile integration was causing numerous data integrity issues, including duplicate records, data inserted into incorrect fields, and the wrong data format being pushed, all

of which required CDK resources to address on behalf of the dealer. In addition, unauthorized third party access was causing significant system performance problems for CDK's dealers.

41. Although Authenticom claims that it actually corrects data-entry errors and anomalies in the data it extracts from CDK's DMS, hostile integrators, like Authenticom, also create errors and anomalies through their unauthorized access to the CDK DMS; errors that have cost CDK substantial amounts of time and money to correct. I don't have any reason to believe that Authenticom does not have the capability to create such errors and anomalies when they hostilely access the CDK DMS.

42. By June 2015, we determined that over 52% of CDK DMSs were infected with "hostile" code and there were at least 27,000 User IDs associated with third-party vendors who were using non-authorized access to pull data from DMS.

43. Concerns that CDK was not getting the full value of the intellectual property that it was delivering to the market also impacted our decision to shut down hostile integration.

44. CDK spent decades and hundreds of millions of dollars creating proprietary software platforms, valuable intellectual property, and an automotive retail data ecosystem of 9,000+ dealers. Defs. Ex. 27.

45. To this day, CDK continues to proactively work to ensure the security of the data on its DMS.

46. In addition to the SecurityFirst program, described in additional detail below, CDK has invested in a variety of other security initiatives, including: (1) keeping all clients on the most current release levels; (2) implementing secure socket layer technology across all DMS applications; (3) developing tools to identify sensitive client information for removal; (4) moving toward unified login credentials for all CDK applications with full auditing capabilities; (5)

adding a new, more secure, suite of dealer data access tools; (6) building a new data transport platform that will become the standard for internal data movement; and (7) creating non-approved data access detection mechanisms that provides dealers with the information needed to better manage their vendor partners.

47. Without a fully secure DMS, CDK would remain "unable to capture full value for our 'CDK Approved' integration due to lack of DMS security." Defs. Ex. 24.

48. With all of the above in mind, in July 2014, I recommended that we take immediate action to secure the DMS to protect data and dealers as part of a broader realignment of the company's Data Services business.

49. To effectively realign the business, I knew we had to simplify the third party access program and "walk the talk" by developing a comprehensive approach to meet the evolving needs of CDK's customers.

50. Our intent was to "[e]xecute a systematic set of engineering, product, and internal initiatives interlaced with assertive marketing programs that increase dealer involvement in dealership data security and severely inhibits hostile integrators from building or maintaining a sustainable business based on access to CDK's DMS[.]" Defs. Ex. 24.

51. The plan, which became known as "SecurityFirst," was not just about keeping hostile integrators out of the DMS (or "locking the box" as its referred to in the industry). Rather our goal was to combine DMS security, new dealer facing tools, more disciplined internal practices and sustained marketing to completely revamp the way CDK approached data security. *Id.* We wanted to achieve this in collaboration with dealers, vendors, and part-and-manufacturer OEMs

52. To achieve this goal we created one plan that applied to all vendors—large and small.

53. SecurityFirst, has four elements: (i) industry transparency and education, (ii) security enhancements to the DMS, (iii) a "refresh" of the 3PA program, and (iv) a new tool for dealers to gain visibility and control over how their data is accessed and used called the Dealer Data Exchange.

54. Although the program didn't officially launch until June 2015, we presented it to the Standards for Technology in Automotive Retail ("STAR") committee of the NADA in October 2014. We also discussed it extensively with industry stakeholders, including dealership GMs and principals, dealer group CIOs, and OEMs. Defs. Ex. 28.

55. One of the critical elements of SecurityFirst was the introduction of new monitoring tools, specifically CDK's Dealer Data Exchange ("DDX"), in October 2015.

56. CDK developed DDX "as a tool to provide dealers with insight into integration." Defs. Ex. 24. __It provides an interface that provides dealers with visibility and control over *all* data connections, including (i) dealer to dealer partner bi-directional third-party integration, (ii) dealer to dealer partner data syndication, (iii) dealer to OEM partner bi-directional integration (DCS), and (iv) dealer to OEM partner data syndication.

57. For this reason, among others, DDX offers dealers more control and visibility over their data in the CDK DMS than Authenticom's "DealerVault" feature purports to offer for data that Authenticom has (without authorization) extracted from the CDK DMS.

58. Using DDX, if a non-authorized connection is detected, dealers are empowered to take a number of steps, including contacting the third party directly, disabling or deleting the third-party's access, and contacting CDK support for further assistance.

59. Importantly, DDX reports also help dealers meet compliance requirements with data security and data safe handling regulations.

60. DDX is available to dealers using CDK's Drive DMS product at no cost. Defs. Ex. 29.

61. As part of SecurityFirst, CDK also implemented increased security enhancements to the DMS.

62. In late 2014, CDK began securing its DMS by removing non-CDK "code on the box," which is known to cause data integrity issues, and disabling user accounts that were recognized as being used for non-approved access. Defs. Ex. 23.

63. Removing the code and blocking unauthorized access served five purposes: (1) it reduced the risk of data corruption and cyber security breaches, (2) it allowed CDK to begin receiving the full value of its intellectual property, (3) it addressed significant system performance issues caused by unauthorized access, (4) it reduced technical support issues created by such access, and (5) it minimized the risk of unauthorized access to protected third party and CDK intellectual property.

64. By Spring 2015, we believed we had performed the necessary due diligence required to ramp up our security efforts and prepare to affirmatively block unauthorized third-party access of the CDK DMS.

65. Hostile integrators, like Authenticom, whose free access to dealer data was interrupted by these increased security measures, and dealers who were not paying for the cost of securing their data, were obviously not happy with the changes and have falsely asserted that CDK's focus on security is just a means of revenue generation.

66. However, there remain a number of DMS companies that have third-party access programs, charging vendors and/or dealers to access DMS platforms and pull or push data, in recognition of the costs of securing the data.

67. Although a decade ago industry leaders, including CDK executives and the NADA, believed DMS providers should not limit third-party access to the DMS because dealers "own" their own data, that does not reflect the state of the industry today.

68. While it is still undisputed that dealer's own their own data, it is now widely recognized that the DMS contains much more than dealer data. That, coupled with the threat of a cyber attack, has led the industry—and CDK—to evolve its approach to DMS access.

69. While CDK does not allow Authenticom (or any other unauthorized third-party) to access its DMS platform outside of the CDK Global Partner program, CDK does not prevent access to dealer data. In fact, one of the main purposes of SecurityFirst and the Third Party Access Plan is to facilitate safe and secure third-party access to dealer data in the DMS.

70. As part of CDK's SecurityFirst initiative, we also undertook a "refresh" of our Third Party Access ("3PA") program.

71. As part of the refresh, CDK expanded the program to include integrations with credit, digital marketing, and financial information previously unavailable to vendors. In addition, data extraction integrations that were previously maintained by running multiple queries throughout the day began to be replaced with "real time" integrations that provided vendors with new data—and only new data—as it was created. These enhancements have improved the ability of third-party vendors to obtain information from the DMS and provide better service to dealers.

72. The refresh also included an update of the pricing model to reflect that security is a shared investment and to create a level playing field for CDK Partner Program participants. Defs. Ex. 23.

73. Prior to 2015 CDK's pricing to vendors varied substantially. The changes to CDK's 3PA pricing structure announced in 2015 were intended to standardize 3PA pricing and eliminate the wide variation in what individual vendors paid for integration. In an effort to provide greater transparency into its programs, CDK publishes it 3PA prices on its website.

74. Additionally, our goal is to offer equivalent to superior DMS and integration functionality at better prices than Reynolds.

75. Another primary driver of the revised pricing was an attempt to recoup costs associated with investment and managing DMS.

76. In evaluating the pricing structure, we reviewed all the costs associated with managing our data-related programs (*e.g.*, enhancing our GSO, certifying vendors, R&D, expanding access by adding new integration points, increased technical support and tools), and determined that the current prices were not fully covering our data-related costs. Data corruption issues caused by unmanaged integration resulted in extremely high support costs and dealer dissatisfaction.

77. Prohibiting unauthorized third-party access to the DMS, including through dealer-issued username and passwords, is an essential component to CDK's third-party access strategy. If CDK enables hostile integrators, it not only will lose critical transparency to data flows in the industry, but it likely will lose participants in the 3PA program. These losses would have real impact—not just financial—on CDK individually and on its dealership community as a whole. The continued development and enhancement of the DMS ecosystem, including strong

participation in the 3PA program, is essential to funding and furthering the evolution of the DMS ecosystem, including the features of the system that keep the data on the DMS secure.

78. Although CDK's evolution and the evolution and innovation of its DMS product is ongoing and by no means complete, if third-parties are granted unfettered access to CDK's DMS, CDK faces an untenable business risk. CDK essentially would have to abandon its current business model and DMS ecosystem strategy and immediately pivot to redirect millions of dollars to redesigning core components of its DMS and instituting new services and support procedures.

I declare under penalty of perjury that the foregoing is true and correct.

Executed in Madison, Wisconsin, this 16th day of June, 2017.

Malcolm Thorne